Jason Lam

BA (CS), CISSP, GCIA, GCFW, GCUX, GCWN, GCIH

E-mail: jason@whitehats.ca

PROFILE:

Jason is an experienced information security professional who is actively involved in the global security community. He frequently speaks at various security events preaching information security to IT professionals with the hopes of improving the current state of the information security field.

Jason also has heavy involvement in the SANS Institute, the most trusted organization in information security. He has written multiple courseware for SANS and is also involved in the GIAC certification process which certify information security professionals.

SKILLS:

- Design secure network with layered perimeter defense systems utilizing various components such as Intrusion Detection System (IDS), filtering routers and firewalls.
- Design, deploy, and monitor IDS.
- Possess extensive knowledge in TCP/IP protocol, network traffic analysis, packet forensics, and OS fingerprinting (passive and active).
- Design and configure IPSec compatible VPN systems.
- Configure and audit security of Unix, Linux Operating Systems and common Internet server software.
- Perform network penetration tests and security assessment.
- Work effectively in a team environment as well as independently.

EMPLOYMENT:

RBC Capital Markets (Royal Bank of Canada) 11/2003-present
Senior Security Analyst/Technical Lead

- Conducted penetration test to reveal vulnerabilities in infrastructure and applications, leading to mitigation of potential security exposures.
- Led the internal effort to handle incidents (worms, virus) and also investigate security incidents, causes of intrusions or security breaches.
- Managed IDS infrastructure with sensors spanning across multiple locations.
- Consulted and collaborated with the internal development team to improve security level in internal customized application.
- Provided security training to IT professionals and also awareness training to non-IT personnel.
- Advised management and the security team of the upcoming threat on the Internet and the risk related to different technologies in use within the Enterprise.
- Participated in the CSIRT (Computer Security Incident Response Team) for the Financial group.

SANS Institute, GIAC certification 2/2002-present
Author / GIAC Certification Lead Grader / Incident Handler (Consultancy)

- Lead author of “Web application security workshop” courseware
- Co-authored the “Cutting-edge hacking technique” courseware
- Perform incident handling duties for Internet Storm Center, one of the most advanced Incident Response team on the Internet. Information provided by this CIRT is used by many government and Fortune 500s for current threat awareness

- Lead an assignment grading team of 11 high profile security professionals across the world, the team consists of professionals from various government agencies, Fortune 500 and consulting companies.
- Accurately and consistently grade the practical assignments written by GCFW (firewall and perimeter defense) and GCIA (Intrusion Analysis) track candidates
- Provide detailed and constructive feedback on each practical paper
- Assisted and provided positive feedback in the continuous development of SANS/GIAC certifications
- Provide training and oversee the progress for new GIAC certification graders
- Contributed course material to SANS GSEC (security essentials) track
- Editor of SANS Windows 2000 Gold Standard material
- Editor of SANS Unix security track material
- Maintainer and editor of SANS Intrusion Detection FAQ document, one of SANS most popular resource on Internet

CGI Inc. 3/2003-10/2003
Security Consultant

Retail chain of a national communication company
Windows XP Desktop Baseline and Hardening service
- Developed a customized Windows XP security configuration template suitable for the specific environment
- Enabled centralized management of security policies on the desktop machines
- Conducted functionality testing and security assessment to verify the impact and effectiveness of the security settings

Financial services company
Security Assessment Services
- Performed security assessment on multiple Cisco IOS routers and PIX firewalls
- Performed host security assessment on multiple Windows NT servers
- Developed recommendations based on industry guidelines to improve the security posture of the Windows NT servers
- Developed a customized Cisco IOS security configuration template suitable for the specific network environment
- Responsible for approving all security related changes on the network prior to deployment

National media company
IDS infrastructure architecture and implementation
- Designed a secure IDS infrastructure on an existing network to monitor and response on network intrusions
- Integrated IDS sensors, reporting consoles and VPN concentrators so all sensors can be monitored by the centralized network operation center at the Managed service provider
- Deployed the IDS sensors and VPN concentrators at client location

Public Services website
Penetration test with custom exploit development
- Developed custom security exploits to attack on multiple security weakness of the web application leading to unauthorized access

Independent Security Consultant 6/2000-2/2003

- Developed defensive strategies, procedures and polices to fit the need of each client
- Actively participated in the design and implementation of network perimeter security architectures with various components such as Firewall, VPN and IDS
- Conducted security assessments and security penetration tests to check for security compliance
- Monitored routers, firewalls and IDS sensors, performed log analysis and event correlation across the organization
- Researched and evaluated current threat levels and advised clients on the current best practices and mitigation methods

World Wide Access, Toronto 5/1999-5/2000
Network Architect

- Planned, rebuilt and maintained the network and servers of a small-medium ISP to improve security. With the implementation of the revised security policy and architecture, hacking incidents were greatly reduced and all illegal attempts were logged.
- Responsible for internal CIRT (Computer Incidents Response Team) duty and assisted Toronto Police on several network incidents.
- Led three junior developers in development of a Voice over IP program using G.723 protocol with C and C++ and completed the project on time.

World Wide Access, Toronto 1/1999-5/1999
Software Developer (Contract)

- Developed a new secure payment module for E-commerce credit card transactions using Java and Perl. This module interfaced with a credit card transaction computer to facilitate online credit card payments on the Web.

EXPERIENCE:

***Vulnerability Scanner**:* Nessus, Retina, SARA, NetIQ Security Analyzer

Firewall: Netfilter, IPFW, IPFilter, Checkpoint, Netscreen, Cisco PIX

VPN: FreeS/Wan, Cisco routers (IOS), Motivus SSL VPN, Nortel Contivity

IDS: Snort, Shadow, Enterasys Dragon, Portsentry

OS: Linux (various distributions since kernel 1.2), Solaris (2.5, 2.7, 8, 9), FreeBSD (4.2+), OpenBSD, Windows NT, 2000 and XP

System Configuration/Auditing Tools: Tcpdump, Tripwire, Logcheck, Bastille, Various password crackers, Nmap

Internet Services and Databases:Apache, Sendmail, Bind, DHCP, LDAP, Qpopper, ProFTP, NFS, MySQL, PostgreSQL, MS SQL, SSH

Programming Languages: C/C++, Java, Perl, PHP

EDUCATION:

York University, Toronto, Ontario
Bachelor of Arts – **Computer Science** Completed in 2001

CERTIFICATION: Certified Information Systems Security Professional (**CISSP**)
SANS GIAC Certified Intrusion Analyst (**GCIA**) – #441 Honor
SANS GIAC Certified Firewall Analyst (**GCFW**) – #281 Honor
SANS GIAC Certified Unix Security Administrator (**GCUX**) – #146 Honor
SANS GIAC Certified Windows Security Administrator (**GCWN**) – Honor
SANS GIAC Certified Incident Handler (**GCIH**) - #530 Honor